(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000181898 A**

(43) Date of publication of application: **30.06.00**

(51) Int. Cl **G06F 15/78**
G06F 12/14

(21) Application number: **10354198**

(22) Date of filing: **14.12.98**

(71) Applicant: **NEC CORP**

(72) Inventor: **OKUDA IKUTARO**

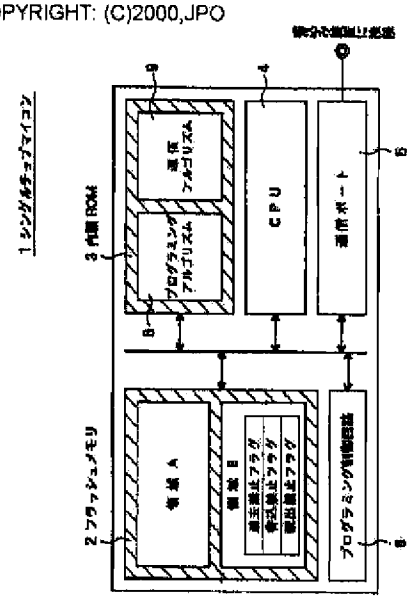
(54) **FLASH MEMORY MOUNTED TYPE SINGLE CHIP MICROCOMPUTER**

COPYRIGHT: (C)2000,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a single chip microcomputer which easily performs write, read and erase management to/from a flash memory about which security measures are considered and has a security function needed for copyright protection, etc.

SOLUTION: This single chip microcomputer 1 consists of a flash memory 2, a built-in ROM 3, a CPU 4, a communication port 5 and a programming controller 6. The memory 2 arranges an area A where programming is performed and an area B for designating a write flag, a read flag and an erase flag which are management information to the area A as pair areas. When a programming request comes from the outside, the CPU 4 refers to the management information of the area B and decides the propriety of executing programming of the area A.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－181898
（P2000－181898A）
(43)公開日　平成12年６月30日(2000.6.30)

(51)Int.Cl.[7]		識別記号	FI			テーマコード（参考）
Ｇ０６Ｆ	15/78	５１０	Ｇ０６Ｆ	15/78	５１０Ａ	５Ｂ０１７
	12/14	３１０		12/14	３１０Ｆ	５Ｂ０６２

審査請求　有　　請求項の数４　ＯＬ　（全６頁）

(21)出願番号　特願平10－354198

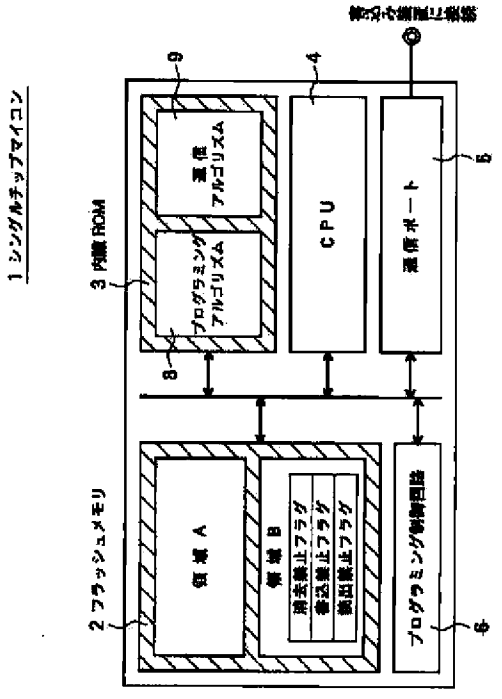
(22)出願日　平成10年12月14日(1998.12.14)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　奥田　郁太郎
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100096231
弁理士　稲垣　清

Ｆターム(参考)　5B017 AA02 AA03 BA04 BB02 BB03
CA12 CA13 CA15
5B062 AA07 CC03 DD10

(54)【発明の名称】　フラッシュメモリ搭載型シングルチップマイクロコンピュータ

(57)【要約】
【目的】　セキュリティ対策が考慮されたフラッシュメモリへの書込み、読出し、及び、消去の管理を容易に行うことができ、著作権保護等のために必要なセキュリティ機能を有するシングルチップマイコンを提供する。
【構成】　シングルチップマイコン１は、フラッシュメモリ２と、内蔵ＲＯＭ３と、ＣＰＵ４と、通信ポート５と、及び、プログラミング制御回路６とで構成されている。フラッシュメモリ２は、プログラミングする領域Ａと該領域Ａへの管理情報である書込みフラグ、読出しフラグ、及び、消去フラグを指定するための領域Ｂとを対領域として配設する。ＣＰＵ４は、外部からのプログラミング要求があると、前記領域Ｂの前記管理情報を参照して前記領域Ａのプログラミングの実行の可否を判断する。



1

【特許請求の範囲】

【請求項１】　フラッシュメモリとマイクロプロセッサとを１の基板上に配設したシングルチップマイクロコンピュータにおいて、

前記フラッシュメモリに第１の領域と該第１の領域のプログラミングの可否を指定するための第２の領域とを配設し、前記マイクロプロセッサは、外部からのプログラミング要求があると、前記第２の領域を参照して前記第１の領域のプログラミングの実行の可否を判断することを特徴とするシングルチップマイクロコンピュータ。

【請求項２】　前記マイクロプロセッサは、前記第１の領域にプログラミングを実行した際に、前記第１の領域のプログラミングを禁止する命令を前記第２の領域に書き込む、請求項１に記載のシングルチップマイクロコンピュータ。

【請求項３】　前記マイクロプロセッサは、前記フラッシュメモリのプログラミングアルゴリズムが記録された、シングルチップマイクロコンピュータ内蔵のＲＯＭによって、前記第２の領域を参照するように制御される、請求項１又は２に記載のシングルチップマイクロコンピュータ。

【請求項４】　前記マイクロプロセッサは、ローダプログラムが記録された、シングルチップマイクロコンピュータ内蔵のＲＯＭによって、前記第２の領域を参照するように制御される、請求項１又は２に記載のシングルチップマイクロコンピュータ。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、フラッシュメモリを搭載したシングルチップマイクロコンピュータに関するものである。

【０００２】

【従来の技術】フラッシュメモリとマイクロプロセッサとを１つのチップに組み込んだフラッシュメモリ搭載型シングルチップマイクロコンピュータ（以下、シングルチップマイコンと呼ぶ）が用いられている。従来のシングルチップマイコンについて、図３を参照して説明する。このシングルチップマイコン１は、フラッシュメモリ２と、通信ポート５と、ＣＰＵ４と、内蔵ＲＯＭ３と、及び、プログラミング制御回路６とから成る各機能部で構成されている。

【０００３】フラッシュメモリ２は、この内部領域を任意の領域（Ａ又はＢ）に分割して管理され、分割した各領域において書込み、読出し、及び、一括消去の各動作が可能である。

【０００４】通信ポート５は、フラッシュメモリ２に対して外部から書込みを行う外部の書込み装置と接続し、書込みデータや専用コマンド等の情報をやり取りする。

【０００５】ＣＰＵ４は、シングルチップマイコン１の全体を管理し、内蔵ＲＯＭ３やフラッシュメモリ２等の

2

プログラムに基づいた処理を実行する。

【０００６】内蔵ＲＯＭ３には、通信ポート５を介してやり取りした情報を受け渡すための手順を記述した通信アルゴリズム９と、フラッシュメモリ２の任意の領域への書込み、読出し、及び、消去を行うための手順を記述したプログラミングアルゴリズム８とが予め格納されている。

【０００７】プログラミング制御回路６は、ＣＰＵ４の制御に基づいてフラッシュメモリ２への実際の書込み、読出し、及び、消去の処理を実行する。

【０００８】シングルチップマイコン１では、プログラミング専用の動作モードにおいて書込み装置から専用コマンドが入力されると、ＣＰＵ４がプログラミングアルゴリズム８中の手順に従ってプログラミング制御回路６を制御することによって、フラッシュメモリ２の任意の領域に対して書込み、読出し、及び、一括消去が実行される。

【０００９】従来のシングルチップマイコン１では、フラッシュメモリ２内の領域への書込み、読出し、及び、消去のプログラミング動作は、専用コマンドで無制限に実行されるため、その実行については書込み装置側に全ての権限が与えられ、フラッシュメモリ２上の情報に対してセキュリティ対策が考慮されていない。この場合、内蔵フラッシュメモリに既に格納されたプログラムの解析や改変等が行われ、ソフトウェアの著作権の保護ができない。

【００１０】特開平４－１７４７７号公報には、ＩＣカードの制御に関する技術が記載されている。図４は、該公報に記載のＩＣカードのデータ構成を示すブロック図である。マイクロコンピュータ２１は内部メモリ２５を有し、内部メモリ２５には、バス線を介して端末装置２８及び外部メモリ２２との間で通信を実行する通信プログラム、通信時の情報が正しいか否かのチェックを行うチェックプログラム、及び、パスワード等の秘密保持を行う秘密保持プログラム等の基本処理プログラムが予め書き込まれている。さらに上記内部メモリ２５のプログラム等によって必要な処理を実行するＣＰＵ２４や、その他インターフェイスが設けられている。

【００１１】マイクロコンピュータ２１と並んで配設された外部メモリ２２は、ＰＲＯＭとして構成され、ユーザの必要な処理を行うプログラムが自由に書き込めるユーザプログラムエリア２６と、所望のデータを書き込むデータエリア２７の２つのエリアを設定してある。

【００１２】内部メモリ２５には、外部メモリ２２内のユーザプログラムエリア２６のアドレスと、データエリア２７の先頭及び最終のアドレスとが予め書き込まれている。従って、ユーザプログラムのロード完了時には、ユーザプログラムエリア２６の最終アドレスにユーザプログラム書込み終了のマークが設定される。

【００１３】そのため、ユーザプログラムエリア２６へ

のユーザプログラムの再ロードの禁止等は、ユーザプログラム書込み終了のマークの有無により行い、データエリア２７への書込み及び読出しの禁止等は、パスワード機能やコードチェックや暗号化することをプログラムとして、ユーザプログラムエリア２６中に作成することで実現していた。

【００１４】

【発明が解決しようとする課題】上記公報に記載の内容は、一般的なＩＰＬ（ＩｎｉｔｉａｌＰｒｏｇｒａｍＬｏａｄｅｒ）機能について述べたものであり、初期的なパーソナルコンピュータで既に実現されているもので、著作権保護等のために必要なセキュリティ機能のために行うデータの扱い方や処理手段は明示されていない。

【００１５】また、外部メモリ２２にＥＥＰＲＯＭを使用した場合には、ブロック単位で電気的消去が可能となるが、上記シングルチップマイクロコンピュータでは、その電気的な消去については記載がない。

【００１６】本発明は、上記したような従来の技術が有する問題点を解決するためになされたものであり、セキュリティ対策が考慮されたフラッシュメモリへの書込み、読出し、及び、消去の管理を容易に行うことができ、著作権保護等のために必要なセキュリティ機能を有するシングルチップマイコンを提供することを目的とする。

【００１７】

【課題を解決するための手段】上記目的を達成するため、本発明のシングルチップマイコンは、フラッシュメモリとマイクロプロセッサとを１の基板上に配設したシングルチップマイクロコンピュータにおいて、前記フラッシュメモリに第１の領域と該第１の領域のプログラミングの可否を指定するための第２の領域とを配設し、前記マイクロプロセッサは、外部からのプログラミング要求があると、前記第２の領域を参照して前記第１の領域のプログラミングの実行の可否を判断することを特徴とする。

【００１８】本発明のシングルチップマイコンによると、書込みフラグ、読出しフラグ、消去フラグの各管理情報を参照することで、該フラッシュメモリへの書込み、読出し、消去の各動作に関する禁止や許可等の管理が容易に行える。

【００１９】本発明のシングルチップマイコンの好ましい態様では、前記第１の領域にプログラミングを実行した際に、前記第１の領域のプログラミングを禁止する命令を前記第２の領域に書き込むことを特徴とする。

【００２０】かかる構成により、プログラムの著作権保護やシステムの安全性保護等の観点から、内蔵のフラッシュメモリ上のソフトウェアの解析や改変を目的とした、フラッシュメモリへの意図的な書込み、読出し、及び、消去のプログラミング動作を任意に禁止できる。

【００２１】前記マイクロプロセッサは、プログラミングの実行の可否を判断するアルゴリズムを、予め内蔵のＲＯＭに記録する構成を採用をすることも、或いは、そのようなアルゴリズムを、内蔵のＲＯＭに予め記録してあるローダプログラムに従って外部からロードする構成を採用をすることもできる。いずれの場合にもプログラミングの実行の可否を判断することが可能になる。

【００２２】

【発明の実施の形態】次に、本発明のシングルチップマイコンが行う、セキュリティ対策が考慮されたフラッシュメモリへの書込み、読出し、及び、消去についての動作を図面を参照して説明する。図１は、本発明の第１の実施形態例のシングルチップマイコンのブロック図である。シングルチップマイコン１は、フラッシュメモリ２と、内蔵ＲＯＭ３と、ＣＰＵ４と、通信ポート５と、及び、プログラミング制御回路６とで構成される。

【００２３】フラッシュメモリ２は予め領域Ａと領域Ｂに分割され、領域Ｂは、領域Ａの管理情報である消去禁止フラグと書込み禁止フラグと読出し禁止フラグとを有する。つまり、領域Ａと領域Ｂは対領域として構成される。フラッシュメモリ２には、このような対領域が複数配設される。

【００２４】内蔵ＲＯＭ３は、通信ポート５を介してやり取りした情報を受け渡すための手順を記述した通信アルゴリズム９と、フラッシュメモリ２の任意の領域を書込み、消去するための手順を記述したプログラミングアルゴリズム８とが、格納されている。

【００２５】ＣＰＵ４は、シングルチップマイコン１を管理し実行する。通信ポート５は、外部の書込み装置と接続し書込みデータや専用コマンド等情報をやり取りする。プログラミング制御回路６は、ＣＰＵ４の制御に基づいて、フラッシュメモリ２への実際の書込み、読出し、及び、消去の処理を実行する。

【００２６】初期状態では、フラッシュメモリ２を構成する個々のメモリセルは消去状態である１を保持している。ＣＰＵ４は、通信アルゴリズム９に従って、通信ポート５を介して外部の書込み装置との間で情報をやり取りする。ＣＰＵ４は、書込み装置からの情報がフラッシュメモリ２の領域Ａに対する書込み、読出し、又は、消去を指示するものである場合には、プログラミングアルゴリズム８に従い、領域Ｂの各フラグを参照してプログラミング制御回路６を制御して領域Ａのためのプログラミング動作を行う。

【００２７】プログラミングが消去動作である場合には、ＣＰＵ４は領域Ｂの消去禁止フラグを参照し、禁止を示す０であれば消去動作を拒否し、許可を示す１であればプログラミングアルゴリズム８に従い、プログラミング制御回路６を制御して領域Ａの消去動作を実行する。

【００２８】プログラミングが書込み動作である場合には、ＣＰＵ４は領域Ｂの書込み禁止フラグを参照し、禁

止を示す０であれば書込み動作を拒否し、許可を示す１であればプログラミングアルゴリズム８に従い、プログラミング制御回路６を制御して領域Ａの書込み動作を実行する。

【００２９】プログラミングが読出し動作である場合には、ＣＰＵ４は領域Ｂの読出し禁止フラグを参照し、禁止を示す０であれば読出し動作を拒否し、許可を示す１であればプログラミングアルゴリズム８に従い、プログラミング制御回路６を制御して領域Ａの読出し動作を実行する。

【００３０】上記実施例によれば、フラッシュメモリへのプログラミング動作を、各領域毎に容易に禁止及び許可ができる。

【００３１】図２は本発明のシングルチップマイコンの第２の実施形態例を示すブロック図である。本実施形態例のシングルチップマイコンは、内蔵ＲＡＭ７を備える点において先の実施形態例とは異なる。

【００３２】内蔵ＲＯＭ３には、通信アルゴリズムとプログラミングアルゴリズムとを、通信ポート５経由で内蔵ＲＡＭ７にダウンロードするための手順を記述したローダプログラム１０が、予め格納されている。

【００３３】初期状態では、フラッシュメモリ２を構成する個々のメモリセルは消去状態である１を保持している。ＣＰＵ４は内蔵ＲＯＭ３に予め格納されたローダプログラム１０を実行し、通信ポート５経由で通信アルゴリズムとプログラミングアルゴリズムを内蔵ＲＡＭ７にダウンロードする。その後、ＣＰＵ４は内蔵ＲＡＭ７に配置された通信アルゴリズム９に従って、通信ポート５を介して外部の書込み装置との間で情報をやり取りする。

【００３４】ＣＰＵ４は、その情報がフラッシュメモリ２の領域Ａに対する書込み、読出し、及び、消去のプログラミング動作を指示する場合には、プログラミングアルゴリズムに従い、領域Ｂの各フラグを参照してプログラミング制御回路６を制御して領域Ａのプログラミング動作を行う。書込み、読出し、及び、消去のプログラミング動作の実際については、第１の実施形態例と同様であるため、その説明を省略する。

【００３５】内蔵ＲＯＭ３は、一般にはマスクＲＯＭとして構成され、例えば製造後にアプリケーション等の関係でプログラミングアルゴリズム及び通信アルゴリズムを変更する等の場合に容易に対応できる。

【００３６】また、上記の第１及び第２の実施形態例のシングルチップマイコンは、上記のプログラミングアルゴリズムの他に、フラッシュメモリ２を全消去状態にできるテストモードを備える。このテストモードは、シングルチップマイコンの製品を出荷する際に、フラッシュメモリをデフォルトとして全消去する際に利用される。

【００３７】

【発明の効果】フラッシュメモリに設定した領域単位で、書込み、読出し、及び、消去のプログラミング動作に関する禁止や許可等の管理を容易に実現することができるので、プログラムの改変や解析等による著作権の侵害を未然に防止できる。この場合、管理する領域単位での禁止や許可等の状態が明確であるため、複数に分割して管理することもできる。

【図面の簡単な説明】

【図１】本発明のシングルチップマイコンの第１の実施形態例を示すブロック図である。

【図２】本発明のシングルチップマイコンの第２の実施形態例を示すブロック図である。

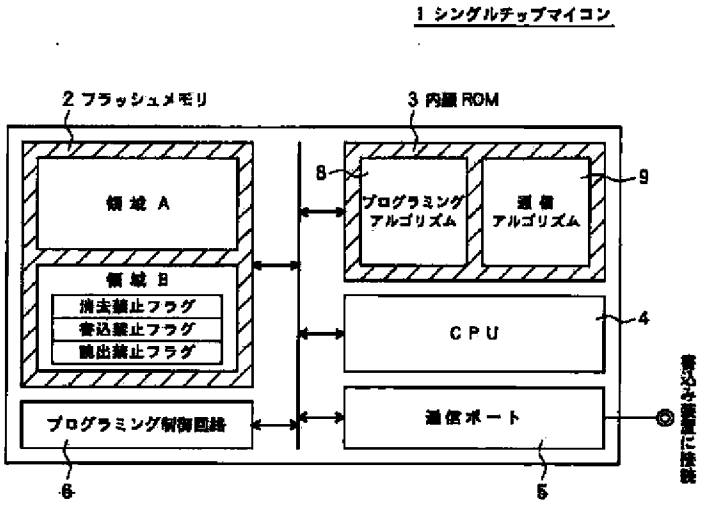
【図３】セキュリティ対策を装備しないシングルチップマイコンを示すブロック図である。

【図４】特開平４－１７４７７号公報に記載のＩＣカードのデータ構成を示すブロック図である。

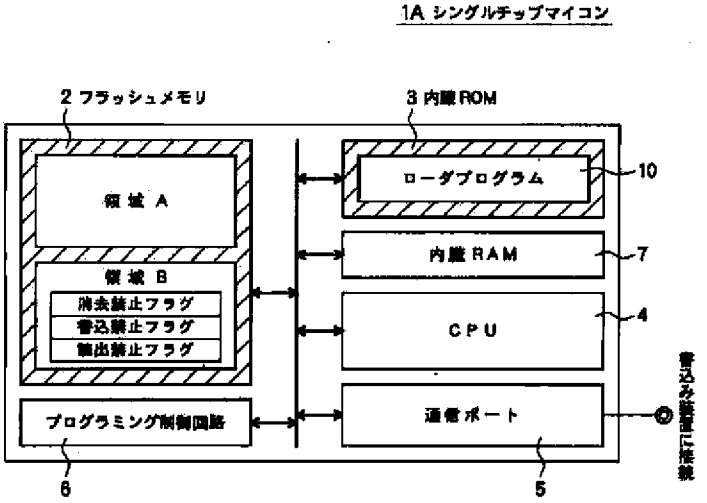
【符号の説明】

１　シングルチップマイコン
２　フラッシュメモリ
３　内蔵ＲＯＭ
４　ＣＰＵ
５　通信ポート
６　プログラミング制御回路
７　内蔵ＲＡＭ
８　プログラミングアルゴリズム
９　通信アルゴリズム
１０　ローダプログラム
２０　ＩＣカード
２１　マイクロコンピュータ
２２　外部メモリ
２３　インターフェイス
２４　ＣＰＵ
２５　内部メモリ
２６　ユーザプログラムエリア
２７　データエリア
２８　端末装置

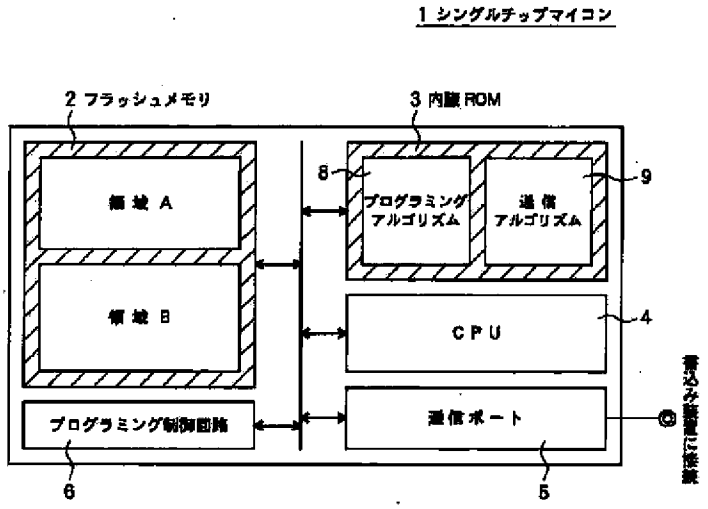
【図１】


1 シングルチップマイコン
2 フラッシュメモリ
3 内蔵 ROM
領 域 A
領 域 B
消去禁止フラグ
書込禁止フラグ
読出禁止フラグ
プログラミング制御回路
8
プログラミング アルゴリズム
通 信 アルゴリズム
9
CPU
4
通信ポート
書込み装置
6
5

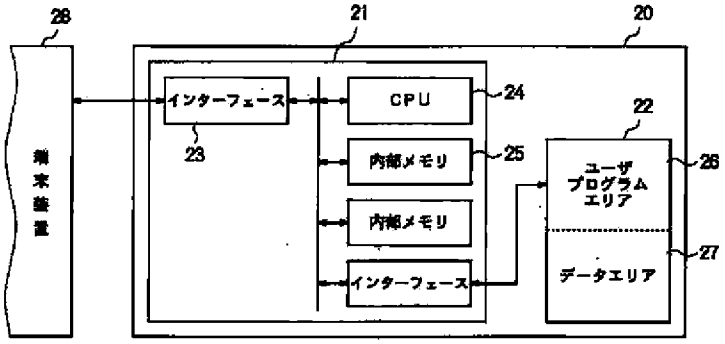
【図２】


1A シングルチップマイコン
2 フラッシュメモリ
3 内蔵 ROM
領 域 A
領 域 B
消去禁止フラグ
書込禁止フラグ
読出禁止フラグ
プログラミング制御回路
ローダプログラム
10
内蔵 RAM
7
CPU
4
通信ポート
書込み装置
6
5

【図３】


1 シングルチップマイコン
2 フラッシュメモリ
3 内蔵 ROM
領域 A
領域 B
8
プログラミング アルゴリズム
通信 アルゴリズム
9
CPU
4
プログラミング制御回路
通信ポート
書込み装置に接続
6
5

【図４】


28
21
20
端末装置
インターフェース
23
CPU
24
内部メモリ
25
内部メモリ
インターフェース
22
ユーザ プログラム エリア
26
データエリア
27